
NimicsCrypt Call
is the best choice to secure your phone calls.

White Paper

Contents

1 Introduction 1
1.1 Characteristics 1
1.2 Design Principle 2
1.3 Security 2
2 Corporate Version 4
3 Retail Version 6

1 Introduction

VoIP (Voice over IP) is a popular technology and has been mass deployed today. The major usage fields can be classified to 3 kinds of applications:

- **Consuming: Skype is the represented application. It's free VoIP software which provides users ultimate talking on internet with free of charge. It also provides service for users to pay to call ordinary PSTN telephones.**
- **PSTN: telecommunication providers use VoIP on public network to connect switch stations and interconnection with other telephony provider.**
- **Corporate: With the progress of better bandwidth and lower cost of internet. More and more communication requirements in corporate are emerged. Microsoft provides a kind of solution for such requirements. It's named Office Communications Server.**
- **Neoi Nimcs provides highly secured VoIP communications since 1998, providing the necessary hardware and Software combination to achieve real Security. Today numerous Corporations, Banks, Security Services, other official Services use the Neoi Nimics Solutions.**

Some of the VoIP services provide encryption options to protect users' privacy. Most of existed solutions are software based security. However, it's meaningless to use software to protect privacy to who needs real secure communication.

Neoi Nimics' NimicsCrypt provides a real hardware solution to protect users' privacy.

1.1 Characteristics

The core value of NimicsCrypt is to provide a secure communication solution with flexible and easy deploying servers.

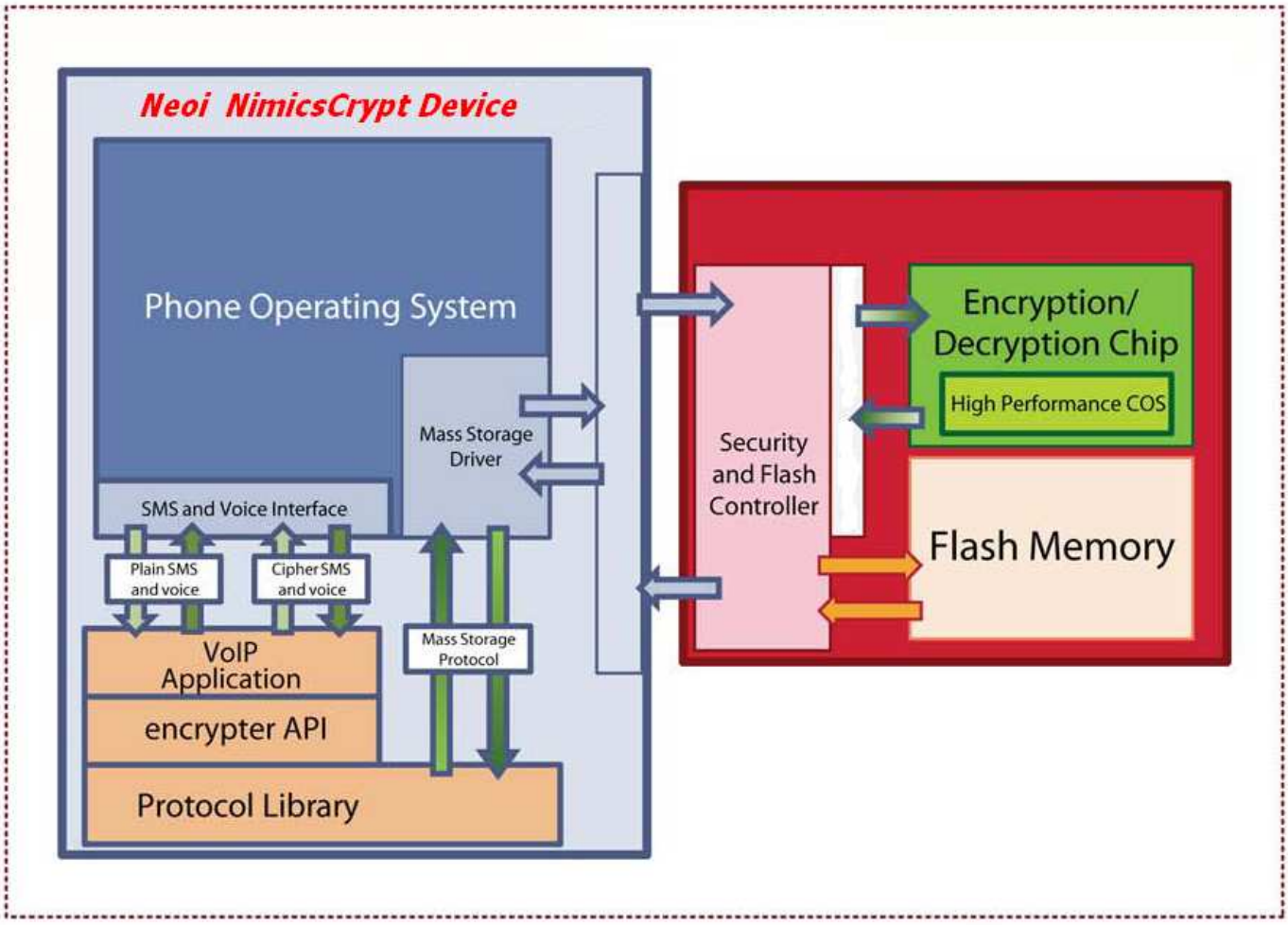
The characteristics of NimicsCrypt solution includes:

- **Mobility: NimicsCrypt client can run on smart phones and other mobile devices.**
- **Extreme Security: All communications data is encrypted and decrypted in certified security chip.**
- **Interoperability: NimicsCrypt solution uses SIP standard to archive best**
- **Robustness: NimicsCrypt servers are passed a set of stress tests and have been deployed on market.**
- **Extensibility and customization: NimicsCrypt corporate version provides a set of optional packages and accepts customization to special requirements.**

1.2 Design Principle

NimicsCrypt is based on existence technology of VoIP which is known as SIP. NimicsCrypt servers are compliant with internal standards.

The security of NimicsCrypt is based on Peer-to-Peer encryption and the client application uses a set of library (encrypted API and GO-Trust Protocol Library) to communicate with NimicsCrypt NeoiChip to build secure tunnel for all voice data and message data over IP network.

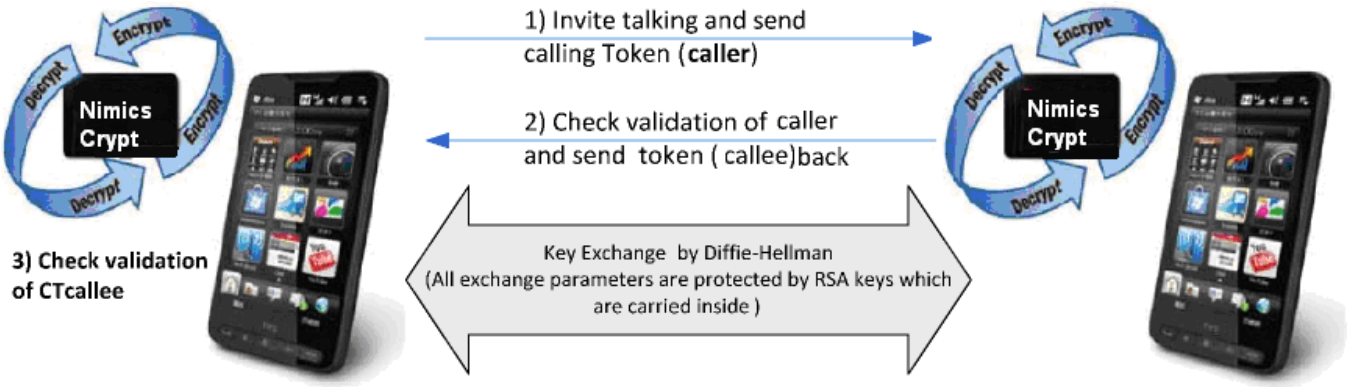


1.3 Security

Security character of NimicsCrypt is as following:

- **Crypto operations: RSA 2048, SHA-256, AES-128.**
- **Security Level: Crypto module inside NIEncrypter certified by Common Criteria EAL 5+ (The level approved by National Security and Banks in many developed countries)**
- **AES throughput supports voice and music.**

- **RSA key pair is generated by encrypted and the private key is never exported.**
- **Voice encryption key (session key) is generated by a True Random Number Generator inside the encrypter and exchanged by RSA and Diffie-Hellman.**
- **Voice is encrypted by the AES-128 session key and the operation is done inside the NIEncrypter.**
- **No confidential keys are stored or computed inside the mobile handset.**
- **Voice encryption key is random and different for each phone call, supporting backward secrecy.**
- **Use proprietary token (Calling Token, CT) which carry user generated RSA public key, SIP ID, and unique serial number inside NimicsCrypt NeoiChip to represent user's identity. Calling token will be taken as elements in key exchange and secure message process.**

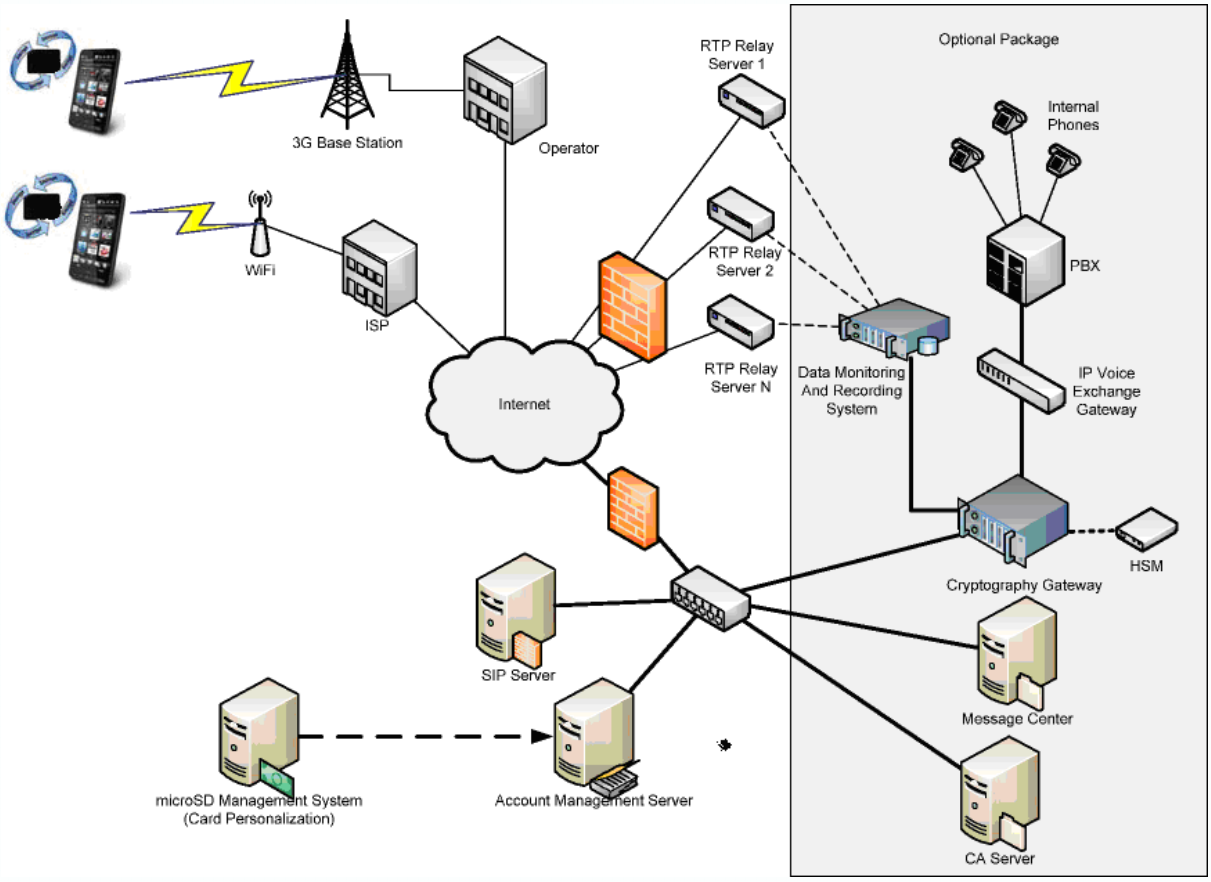


Build Secure Voice Tunnel Process

Note: The process of building secure voice could be changed in corporate version according to customization requirements.

Secure Message Process

2 Corporate Versions



Standard Package

☐ **SIP Server: Provide following 2 functionalities.**

o SIP Registration: The user registration process complies with SIP protocol standard. Phone number assignment rule can be customized flexibly.

o Secure Call and Message Handling: This server handles the secure call request from NimicsCrypt client and redirects the call to another client. This server will then setup Peer-to-Peer tunnel between 2 NimicsCrypt clients. This server also handles secure message process.

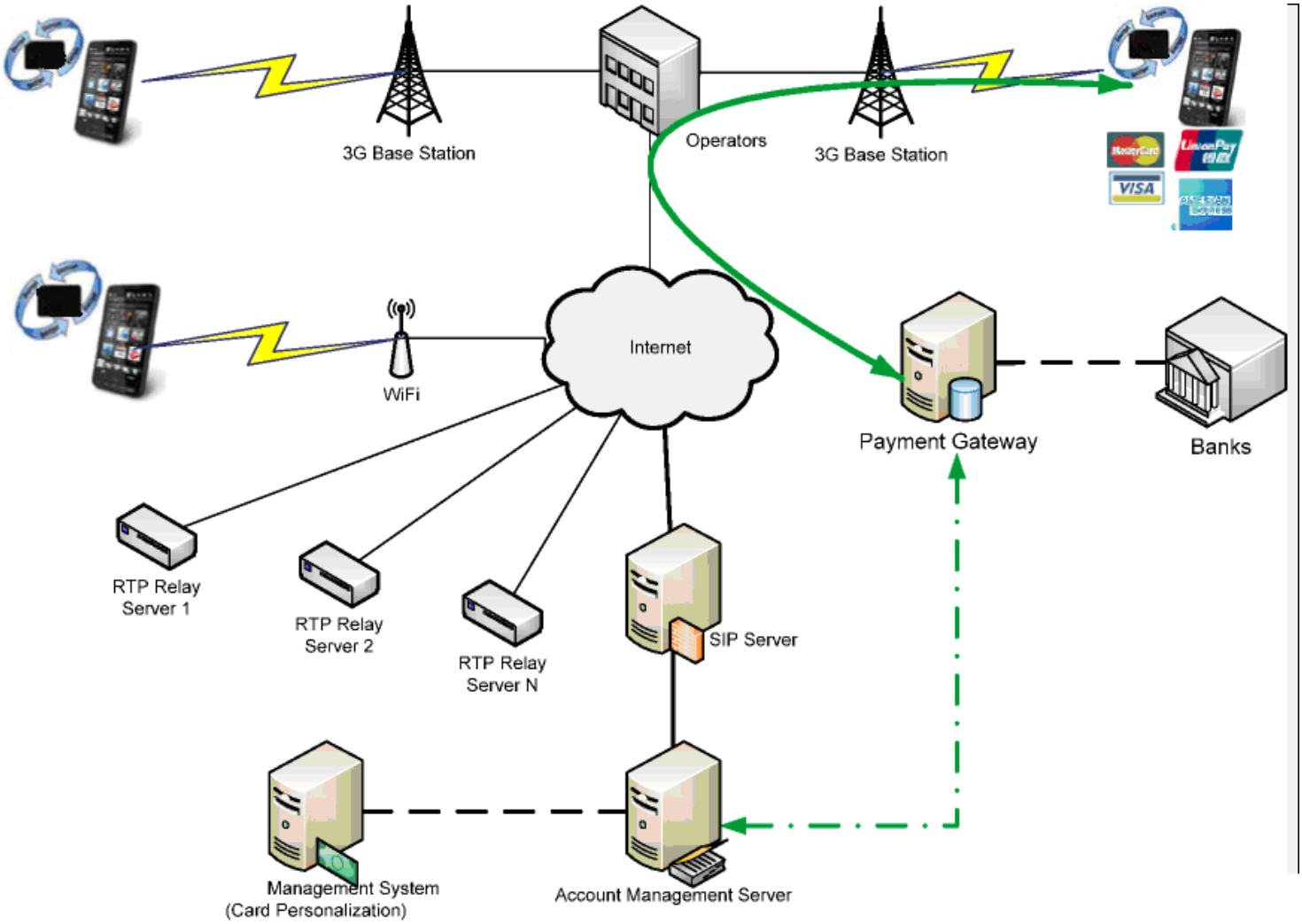
- User Account Management: Set user authority according to the account information from Account Management Server.
- Network Statics Management: Manage the network statics information which includes user logon/logoff statics, user communication load analysis, RTP relay load statics, and RTP relay load warning mechanism.
- Real time status audit /log management: Server can generate report or acknowledgement for real time status.
- RTP Relay Server: All voice data will be forwarded by RTP server to insure transmission quality.
- Account Management Server: This server may the same with SIP server. All users' accounts will be managed bythis server.
- NimicsCrypt NeoiChip Management System: This is a standalone machine with a personalization toolset. Administrator can initialize NimicsCrypt NeoiChip on this server: System keys/certificate, User keys/certificate, SIP Server address (domain name), SIP number, SIP account, etc.

Optional Package

- CA Server: The standard PKI mechanism is optional in corporate version.
- Message Center: Broadcast encrypted text message or pictures to every NimcsCrypt clients. Manage system notification to all users and send control messages to change data in NimicsCrypt NeoiChip or remotely destroy NimicsCrypt NeoiChip.
- Cryptographic Gateway: When user uses mobile phone to call internal landline, cryptographic gateway will be in charge of establish secure tunnel with user. Besides, this gateway can also be used for data record system to decrypt communication data.

- **HSM: Hardware Security Module. This module is in charge of cryptographic operations and key storage.**
- **IP Voice Exchange Gateway: External call will be transfer to PSTN phone by this gateway.**

3 Retail Version



In retail version, NimicsCrypt system invokes the standard package of corporate version and a payment system for users to pay monthly to get authorization of using NimicsCrypt service.